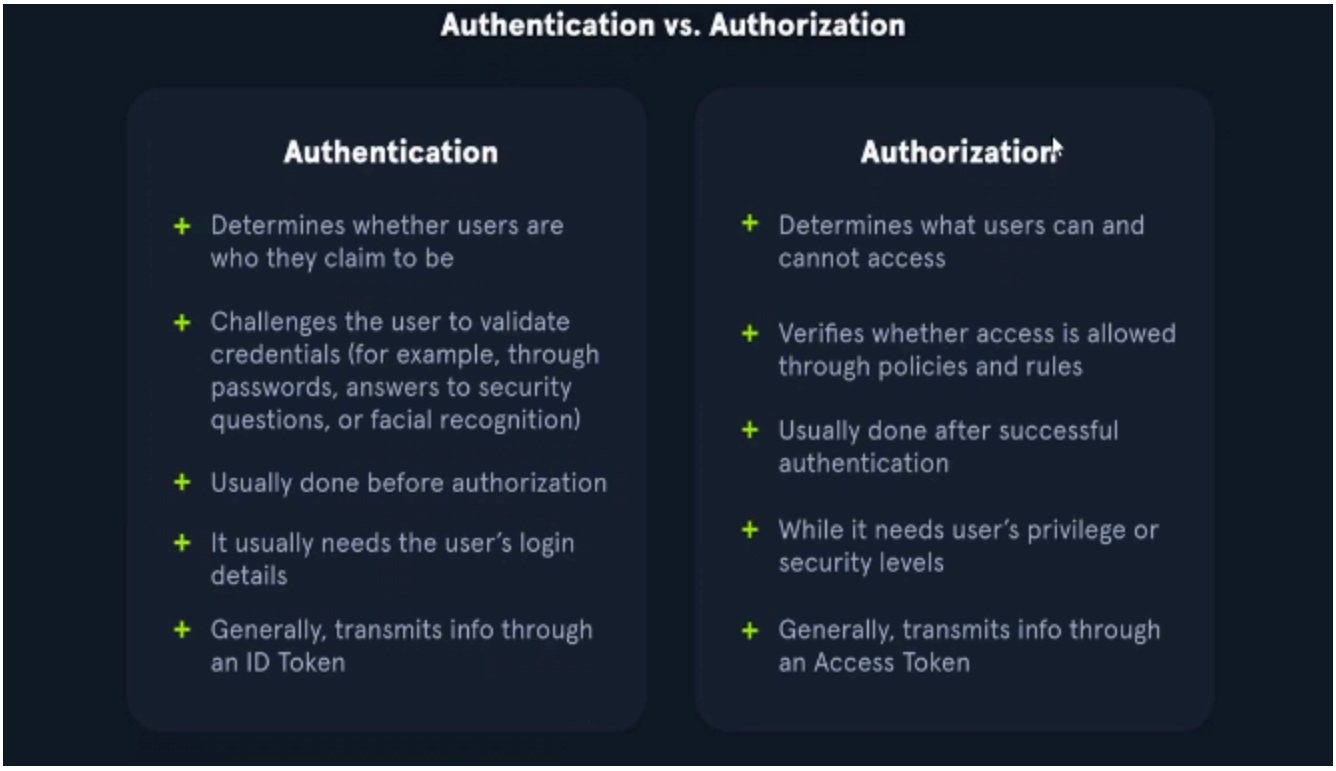
broken access control



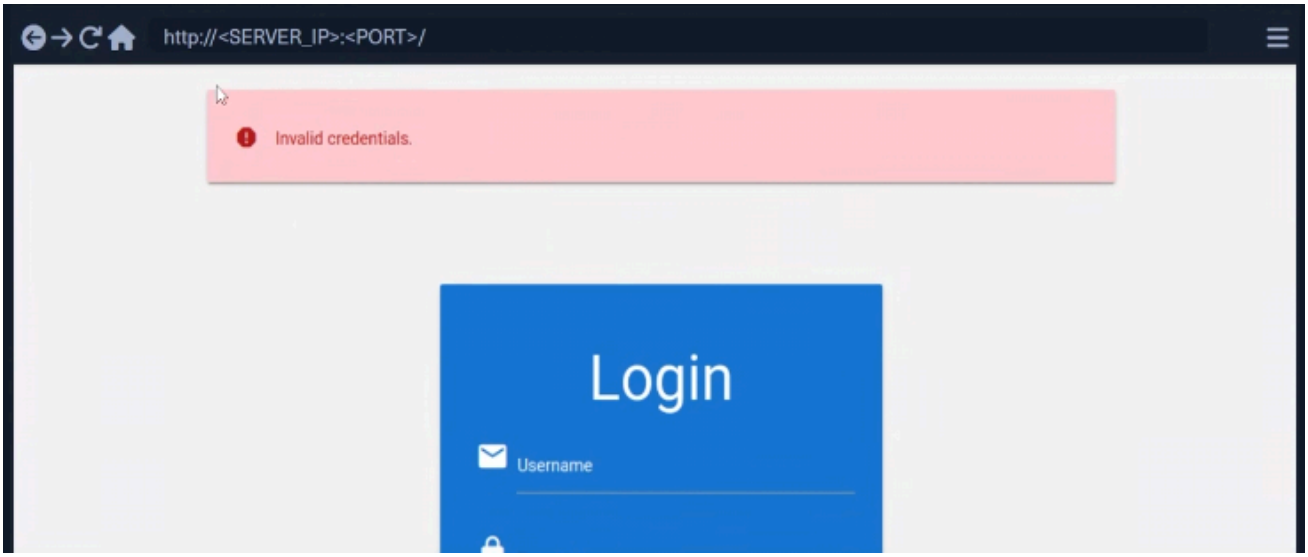
- هنا اول حاجه تعرف الفرق بين authentication authorization

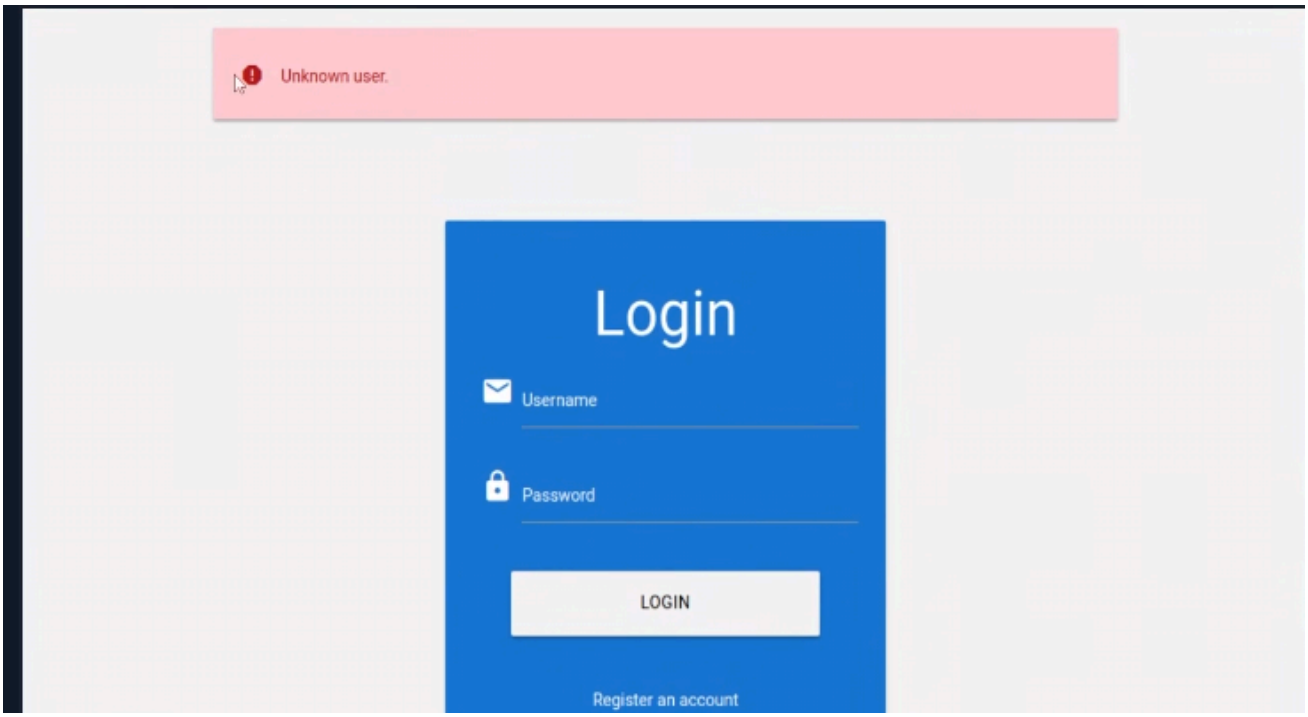
Authentication

- بتتأكد إن المستخدم هو فعلاً الشخص الطلوب
- بتطلب من المستخدم يثبت هويته (زي الباسورد، سؤال أمان، بصمة، أو بصمة الوجه)
- دايمًا بتحصل **قبل** التفويض (Authorization)
- بتحتاج بيانات دخول المستخدم (زي اليوزر نيم والباسورد)
- بتنقل البيانات غالبًا باستخدام **ID Token**

Authorization

- بتحدد إيه اللي المستخدم يقدر يعمله أو يوصله
- بتراجع السياسات والقواعد علشان تشوف المستخدم له صلاحية ولا لأ.
- بتحصل **بعد** ما المستخدم يتأكد هويته (يعني بعد الـ Authentication).
- بتعتمد على صلاحيات المستخدم أو مستوى الأمان الخاص بيه.
- بتنقل البيانات غالبًا باستخدام **Access Token**.

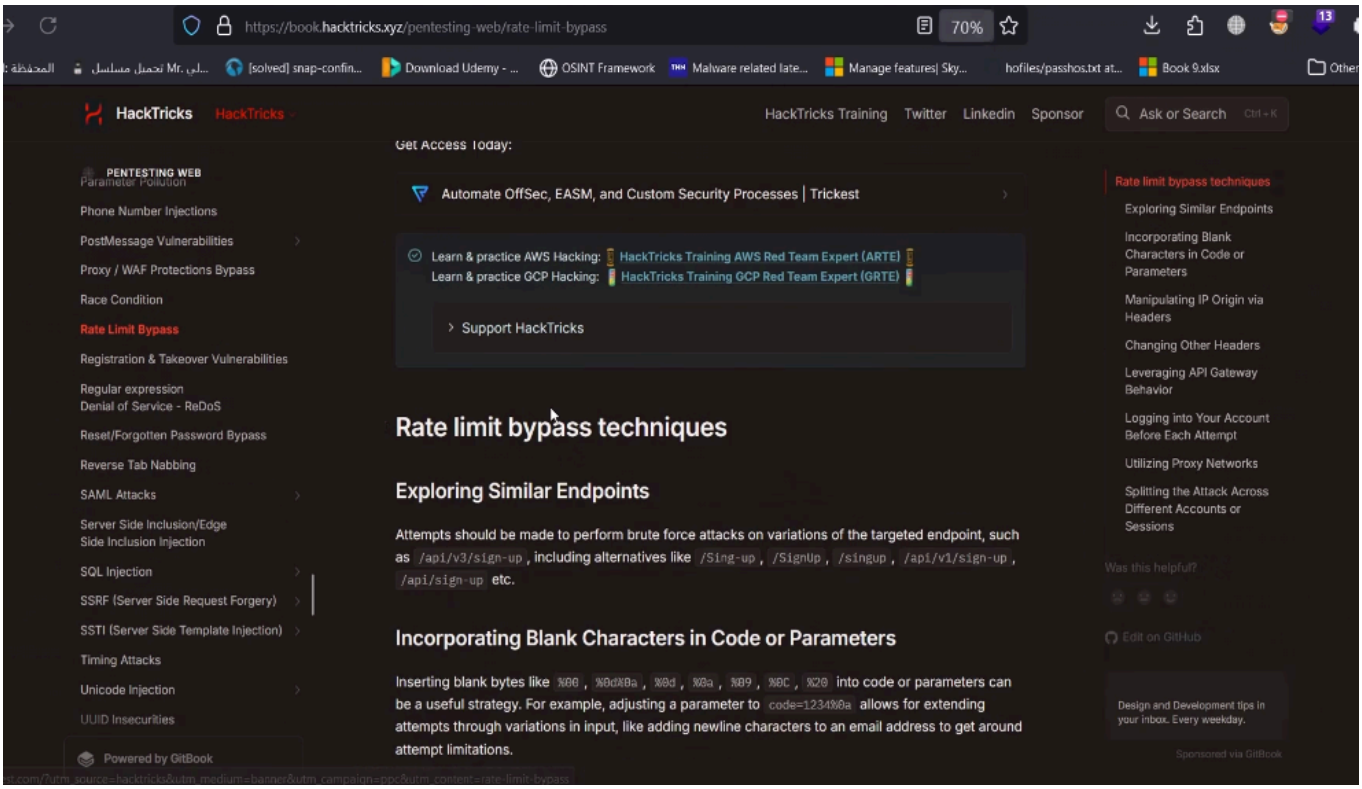




- هنا ممكن تلاحظ فرق في error
- دي ممكن تكون ثغره عشان نت كدا قدرت تعمل enumeration user

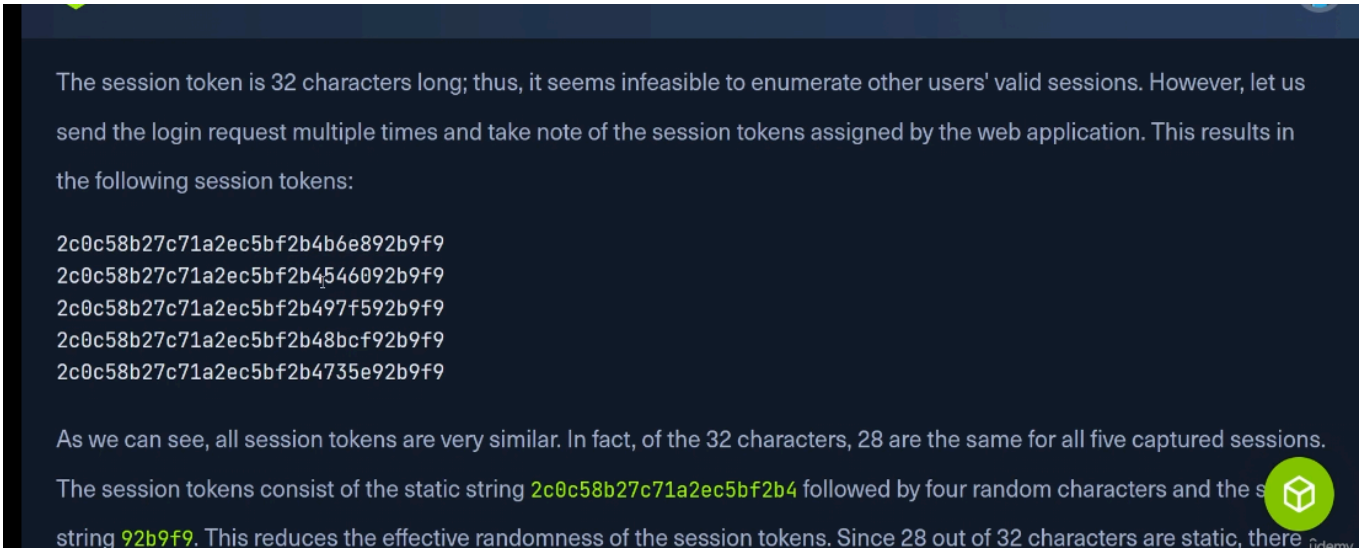
```
root@team:~/wordlist/SecLists/Usernames# ffuf -u http://83.136.255.196:49534 -w xato-net-10-million-usernames.txt -d "username=FUZZ&password=oifjaojad" -H "Content-Type: application/x-www-form-urlencoded" -X POST
```

- تستعمل ffuf عشان تعمل fuzz بالطريقه دي



- دا موقع اسمه hack tricks
- بيساعدك انه يديك حاجات تعدي بيها rate limit

- ممكن تلاقي ثغره في captha عن طريق انه هي بتكون id نفسه تعتبر ثغره



- ممكن لو لقيت session مشتابهه كدا الول اختلاف بسيط
- ممكن تفكه عادي تعمله decode وتكسره